

ABSTRACT OF THE DISCLOSURE

An operating system copies data from memory pages into a paging file on disk, in order to free up space in the memory. A mechanism is disclosed that causes the data to be encrypted as it is copied into the paging file, thereby protecting the paged data from unauthorized (or otherwise undesired) observation. The data that is stored in the paging file is encrypted with a session key, that is generated shortly after the machine on which the paging file exists is started. The session key, which is used both for encryption and decryption of the paging file data, is stored in volatile memory, so that the key is not persisted across boots of the machine. Since the key is not persisted across boots, old paging file data that was stored prior to the most recent boot cannot be recovered in clear text, thereby protecting the data from observation.